V3.0 FortiGate-3000/FortiGate-3600
设备安装手册

www.fortinet.com

V3.0 FortiGate-3000 /FortiGate-3600 设备安装手册

2005年12月12日
01-30000-0270-20051212

注册商标

动态威胁防御系统（DTPS），APSecure, FortiASIC, FortiBIOS, FortiBridge, FortiClient, FortiGate,FortiGate 统一威胁管理系统，FortiGuard, FortiGuard-Antispam, FortiGuard-Antivirus, FortiGuard-Intrusion, FortiGuard-Web, FortiLog, FortiManager, Fortinet, FortiOS, FortiPartner, FortiProtect, FortiReporter, FortiResponse, FortiShield, FortiVoIP 和 FortiWiFi 均是飞塔有限公司的注册商标（包括在美国和在其他国家的飞塔有限公司）。
本手册中提及的公司和产品由他们各自的所有者拥有其商标或注册商标。

服从规范

FCC Class A Part 15 CSA/CUS

⚠ **注意：**如果您安装的电池型号有误，可能会导致爆炸。请根据使用说明中的规定处理废旧电池。

目录

简介

欢迎选购Fortinet产品构筑实时网络防护。

FortiGate ™ 统一威胁管理系统增强了网络的安全性，避免了网络资源的误用和滥用，帮助您更有效的使用通讯资源的同时不会降低网络的性能。FortiGate病毒防火墙获得了ICSA 防火墙认证，IP 安全认证和防病毒服务认证。

FortiGate统一威胁管理系统是致力于网络安全的，易于管理的安全设备。其功能齐备，包括：
- 应用层服务，例如病毒防护和内容过滤，
- 网络层服务，例如防火墙、入侵检测、VPN以及流量控制等。

FortiGate统一威胁管理系统采用了先进的行为加速（Accelerated Behavior）和内容分析系统技术（ABACASTM），具有芯片设计、网络通信、安全防御及内容分析等方面诸多技术优势。独特的基于ASIC上的网络安全构架能实时进行网络内容和状态分析，并及时启动部署在网络边界的防护关键应用程序，随时对您的网络进行最有效的安全保护。

Fortinet 产品家族

Fortinet 的产品家族涵盖了完备的网络安全解决方案包括邮件，日志，报告，网络管理，安全性管理以及FortiGate 统一安全性威胁管理系统的既有软件也有硬件设备的产品。

更多Fortinet产品信息，详见 www.fortinet.com/products .

FortiGuard服务订制

FortiGuard 服务定制是全球Fortinet安全专家团队建立,更新并管理的安全服务。Fortinet安全专家们确保最新的攻击在对您的资源损害或感染终端用户使用设备之前就能够被检测到并阻止。FortiGuard服务均以最新的安全技术构建，以最低的运行成本考虑设计。

FortiGuard 服务订制包括：
- FortiGuard 反病毒服务
- FortiGuard 入侵防护（IPS）服务
- FortiGuard 网页过滤服务
- FortiGuard 垃圾邮件过滤服务
- FortiGuard Premier伙伴服务

并可获得在线病毒扫描与病毒信息查看服务。

FortiClient

FortiClient ™ 主机安全软件为使用微软操作系统的桌面与便携电脑用户提供了安全的网络环境。FortiClient的功能包括：

- 建立与远程网络的VPN连接
- 病毒实时防护
- 防止修改Windows注册表
- 病毒扫描

FortiClient还提供了无人值守的安装模式，管理员能够有效的将预先配置的FortiClient分配到几个用户的计算机。

FortiMail

FortiMail ™安全信息平台针对邮件流量提供了强大且灵活的启发式扫描与报告功能。FortiMail单元在检测与屏蔽恶意附件例如DCC（Distributed Checksum Clearinghouse）与Bayesian扫描方面具有可靠的高性能。在Fortinet卓越的FortiOS与FortiASIC技术的支持下，FortiMail反病毒技术深入扩展到全部的内容检测功能，能够检测到最新的邮件威胁。

FortiAnalyzer

FortiAnalyzer ™ 为网络管理员提供了有关网络防护与安全性的信息，避免网络受到攻击与漏洞威胁。FortiAnalyzer具有以下功能：

- 从FortiGate与syslog设备收集并存储日志。
- 创建日志用于收集日志数据。
- 扫描与报告漏洞。
- 存储FortiGate设备隔离的文件。

FortiAnalyzer也可以配置作为网络分析器用来在使用了防火墙的网络区域捕捉实时的网络流量。您也可以将FortiAnalyzer用作存储设备，用户可以访问并共享存储在FortiAnalyzer硬盘的报告与日志。

FortiReporter

FortiReporter™安全性分析软件生成简洁明的报告并可以从任何的FortiGate设备收集日志。FortiReporter可以暴露网络滥用情况，管理带宽，监控网络使用情况，并确保员工能够较好的使用公司的网络。FortiReporter还允许IT管理员能够识别并对攻击作出响应，包括在安全威胁发生之前先发性的确定保护网络安全的方法。

FortiBridge

FortiBridge™产品是设计应用于当停电或是FortiGate系统故障时，提供给企业用户持续的网络流量。FortiBridge绕过FortiGate设备，确保网络能够继续进行流量处理。FortiBridge产品使用简单，部署方便；您可以设置在电源或者FortiGate系统故障发生的时FortiBridge设备所应采取的操作。

FortiManager

FortiManager™系统设计用来满足负责在许多分散的FortiGate安装区域建立与维护安全策略的大型企业（包括管理安全服务的提供商）的

需要。拥有该系统，您可以配置多个FortiGate并监控其状态。您还能够查看FortiGate设备的实时与历史日志，包括管理FortiGate更新的固件镜像。FortiManager 系统注重操作的简便性包括与其他第三方系统简易的整合。

关于FortiGate设备

FortiGate-3000与FortiGate-3600病毒防火墙设备所提供的承载级性能与可靠性，能够满足大型企业和服务商的需求。
FortiGate-3000与FortiGate-3600设备还备有冗余电源，减少了单向故障包括负载平衡操作与冗余故障，不间断运行。FortiGate-3000的高性能、可靠性与易于管理特点使其成为网络管理服务的理想选择。

FortiGate-3000

FortiGate-3000病毒防火墙设备所提供的承载级性能与可靠性，能够满足大型企业和服务商的需求。
该设备应用了多个CPU与FortiASIC芯片技术能够提供3Gbp的吞吐量，满足了大部分要求比较严格应用的需要。

FortiGate-3000设备还备有冗余电源，减少了单向故障包括负载平衡操作与冗余故障。FortiGate-3000的高性能、可靠性与易于管理特点使其成为网络管理服务的理想选择。

FortiGate-3600

FortiGate-3000病毒防火墙设备所提供的承载级性能与可靠性，能够满足大型企业和服务商的需求。
该设备应用了多个CPU与FortiASIC芯片技术能够提供4Gbp的吞吐量，满足了大部分要求比较严格应用的需要。

FortiGate-3600设备还备有冗余电源，减少了单向故障包括负载平衡操作与冗余故障。FortiGate-3600的高性能、可靠性与易于管理特点使其成为网络管理服务的理想选择。

关于本手册

该文档就如何安装FortiGate设备，在网络中配置设备，以及如何安装与升级固件进行了说明。

该手册包含以下章节：
- 安装FortiGate设备— 安装并启动FortiGate设备。
- 出厂默认设置 — FortiGate设备出厂默认设置信息。
- 在网络中配置FortiGate设备 — FortiGate设备的操作模式说明以及如何将FortiGate设备集成到网络中。

• FortiGate固件 — 描述了如何安装，升级，恢复与测试FortiGate设备的固件。

该手册中的注释

以下是该手册中的注释：
- 在所举的例子中，私人IP地址既可以用做私人也可以是公共IP地址。
- 注意与警告标识中的提示较为重要的信息。


注意：突出另外其它的有用信息。


警告：对可能造成意外的不良的结果包括数据丢失或者设备损害等命令或程序发出警告提示。

排版说明

以下是该安装手册中使用的排版说明：

排版说明	举例
键盘输入	在网关名称字段，键入远程VPN或用户（例如，Central_office_1）
命令举例	Config sys global Set ips-open enable end
CLI命令句法模式	Config firewall policy edit id_integer set http_retry_count <retry_interer> set natip <address_ipv4mask> end
文档名称	*FortiGate管理员使用手册*
菜单命令	进入 VPN>IPSEC>阶段1并点击新建。
程序输出	Welcome!
变量	<address_ipv4>

FortiGate技术文档

您可以从Fortinet技术文档网站http://kc.forticare.com，获得最新发布的Fortinet技术文档。

公开以下Fortinet产品技术手册：
- *FortiGate快速启动指南*

提供关于连接与安装Fortinet设备的信息。
- *FortiGate设备安装手册*

提供有关如何安装FortiGate设备的信息。包括硬件信息,默认配置信息，安装操作，连接操作以及基本的配置操作。请查看产品型号选择不同的安装手册。

• *FortiGate管理员使用手册*

有关如何配置FortiGate设备的基本信息，包括如何定义FortiGate病毒防护与防火墙策略；如何应用入侵保护，病毒防护，网页内容过滤以及垃圾邮件过滤服务与配置VPN。

• *FortiGate在线帮助*

在线帮助是对FortiGate管理员手册的HTML格式上下文有关的检索与查询。您可以通过基于web的管理其访问在线帮助。

• *FortiGate CLI参考手册*

有关如何使用FortiGate CLI（命令行接口）以及所以FortiGateCLI命令的参考。

• *日志信息参考手册*

访问Fortinet公司网站的Fortinet知识库板块，FortiGate 日志信息参考对FortiGate日志信息的结构与FortiGate设备所生成的日志信息有关内容做了描述。

• *FortiGate HA 用户使用指南*

深入介绍了FortiGate 高可用性的性能与FortiGate群集协议的信息。

• *FortiGate IPS 用户使用指南*

对如何配置FortiGate设备的入侵检测功能以及IPS是如何处理普通的攻击做出了描述。

• *FortiGate IPSec VPN 用户指南*

对使用基于web的管理器如何配置IPSec VPN进行了逐步详细的说明。

• *FortiGateSSL VPN 用户使用指南*

对FortiGate IPSec VPN与FortiGate SSL VPN 技术进行比较，并对通过基于web的管理器,远程用户怎样配置只适用于网络模式与通道模式SSL VPN访问做了描述。

• *FortiGate PPTP VPN 用户使用指南*

使用基于web的管理器如何配置PPTP VPN。

• *FortiGate Certificate Management User Guide证书管理用户指南*

管理电子证书的程序包括生成电子证书的请求，安装签发的证书，引入CA根权威证书与证书撤销名单，以及备份与存储安装的证书信息与私人密钥。

• *FortiGate VLAN and VDOM 用户使用指南*

在NAT/路由与透明模式下如何配置VLAN与VDOM。

Fortinet 知识库

其它有关Fortinet技术手册信息都可以从Fortinet公司网站（www.fortinet.com)中的知识库板块获得。知识库涵盖涉及fortinet产品故障排除与解释说明性的文章，FAQ，技术说明等。

Fortinet 技术文档的建议与意见

如果您在本文档或任何Fortinet 技术文档中发现了错误或疏漏之处，欢迎您将有关信息发送到 techdoc@fortinet.com 。

客服与技术支持

Fortinet 技术支持将确保您的Fortinet系统在您的网络中能够快速启动，轻松配置并能够可靠运行。
敬请访问Fortinet技术支持网站http://support.fortinet.com 获知更多Fortinet所提供的技术支持服务。

FortiGate设备安装

本章节就如何安装以及在网络中配置FortiGate设备进行了详细说明。具体包括：

设备包装

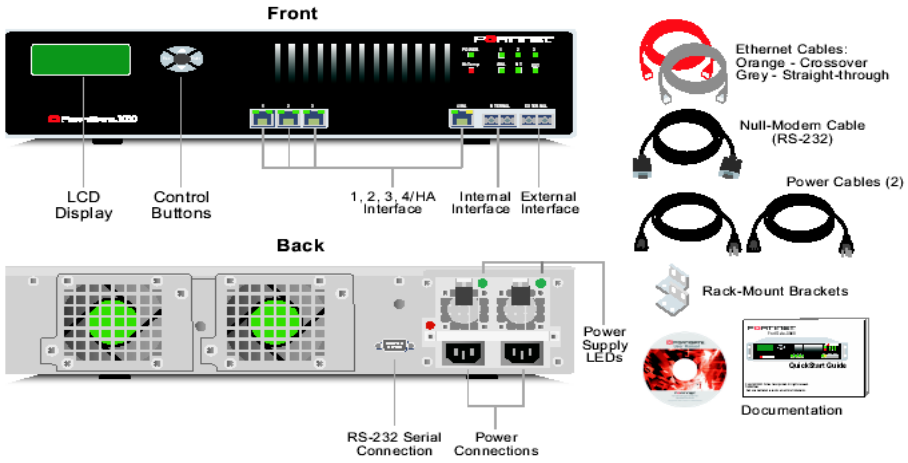
请检查FortiGate设备包装盒所有部件。

FortiGate-3000

FortiGate-3000设备包装盒中部件：

- FortiGate-3000防火墙设备
- 一根橙色以太网交叉线缆（Fortinet 部件号：CC300248）
- 一根灰色以太网普通线缆（Fortinet 部件号：CC300249）
- 一根交叉MODEM线（Fortinet 部件号：CC300247）
- 两个19英寸大小的安装架
- 两根电源线
- FortiGate-3000设备快速启动指南册页
- Fortinet技术手册CD一张

图1：FortiGate-3000设备部件



安装

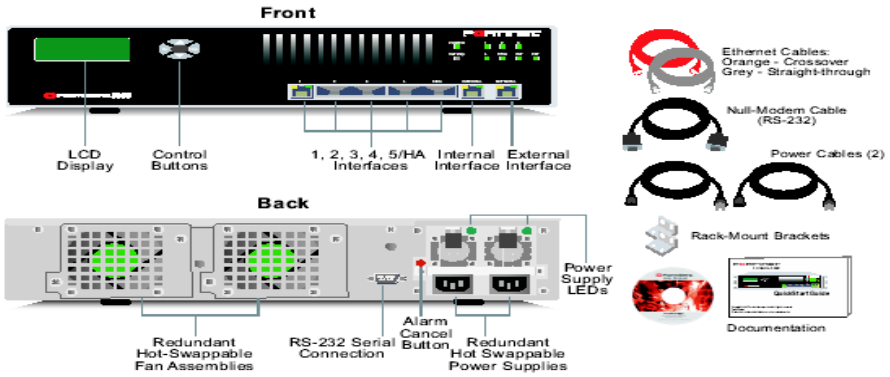
FortiGate-3000可以固定在标准的19英寸的机架上。需要占据机架2 U的垂直空间。FortiGate-3000设备也可作为独立的器件放置在任何水平的表面。

表1：技术参数

尺寸	16.75×13.5×3.5英尺 （42.7×33×8.9厘米）
重量	17.5磅 （8千克）
功率	最大功率：360W
工作需求	AC输入电压：100至240VAC AC输入电流：6A 频率：50至60Hz • FortiGate-3000可能会对供电电路造成负载，或对过电流保护造成影响。请用适当名牌标注该影响。 • 确保FortiGate-3000有接地线。Fortinet公司建议与支路直接连接。
工作环境说明	工作温度：32至104华氏度（0至40度摄氏度） 放置温度：－13至158华氏度 （－25至70摄氏度） 湿度：5至95% （非冷凝）

FortiGate-3600

- FortiGate-3600防火墙设备
- 一根橙色以太网交叉线缆（Fortinet部件号）
- 一根灰色以太网普通线缆（Fortinet 部件号：CC300249）
- 一根交叉MODEM线（Fortinet 部件号：CC300247）
- 两个19英寸安装架
- 两根电源线
- FortiGate-3600设备快速启动指南册页
- Fortinet技术手册CD一张



安装

FortiGate-3600可以固定在标准的19英尺的机架上。需要占据机架2 U的垂直空间。FortiGate-3600设备也可作为独立的器件放置在任何水平的表面。

表2：技术参数

尺寸	16.75X13.5X3.5英尺 （42.7X33X8.9厘米）
重量	17.5磅 （8千克）
功率	最大功率：460W
工作需求	AC输入电压：100至240VAC AC输入电流：6A 频率：50至60Hz • FortiGate-3600可能会对供电电路造成负载，或对过电流保护造成影响。请用适当名牌标注该影响。 • 确保FortiGate-3000有接地线。Fortinet公司建议与支路直接连接。
工作环境说明	工作温度：32至104华氏度（0至40度摄氏度） 放置温度：－13至158华氏度 （－25至70摄氏度） 湿度：5至95％ （非冷凝）

空气流通

• 机架安装时，确保有一定的空气流量与通风以便FortiGate设备能够正常工作。
• FortiGate-3600独立安装时，确保FortiGate设备周边至少有15英寸（3.75厘米）的距离，有足够的空气流通与冷却。
• 如果将FortiGate设备安装在邻近的或多重机架的组合中，机架周边的工作环境温度将会高于工作间的温度。确保工作环境温度不超过设备制造商规定的工作温度。

机械性负荷

进行机架安装时，确保FortiGate设备的机械性负荷平均分担避免发生危险。

启动FortiGate设备

FortiGate设备中不设ON/OFF开关。

启动FortiGate设备

1. 将电源线与位于FortiGate设备背面的电源接口连接。
2. 将电源线连接到电源插座。

每根电源线都应该连接到不同的电源。如果一个电源发生故障，其它的仍可正常运行。

数秒后，LED显示SYSTEM STARING（系统启动）。

系统启动后，LED显示Menu（主菜单）。

FortiGate设备开始运行，LED指示灯亮起。FortiGate设备启动过程中LED状态指示灯闪烁并在设备启动后保持亮着状态。

表3：LED显示

LED	状态	描述
Power	绿色	FortiGate设备启动。
	熄灭	FortiGate设备断电。
1，2，3，4， 4/HA，5/HA， INT，EXT	绿色	连接线使用正确，连接的设备已启动。
	绿色闪烁	此接口有网络活动。
	熄灭	没有连接建立。
1，2，3 （接口） （10/100 接口）	绿色	连接线使用正确，连接的设备已启动。
	绿色闪烁	此接口有网络活动。
	绿色	此接口已建立速率为100Mbps的连接。
	熄灭	没有连接建立。
内部，外部 （千兆缆线接口） 4/HA 接口	橙色	连接线使用正确，连接的设备已启动。
	橙色闪烁	此接口有网络活动。
	绿色	此接口已建立速率为100Mbps的连接
	熄灭	没有连接建立。

注意：如果只连接一个电源，有声报警将指示电源故障。按下设备后面电源旁边的红色报警取消键停止报警。

注意：LED指示灯位于设备正面右上角。

关闭FortiGate设备

请在闭合电源开关之前，关掉FortiGate操作系统，以免造成硬件损伤。

关闭FortiGate设备

1. 访问基于web的管理器，进入系统> 系统状态> 系统状态，选择关闭系统，然后点击“确认”关闭系统；或者在命令行接口（CLI）中，输入execute shutdown
2. 将电缆线从电源连接处拔掉。

连接FortiGate设备

有三种方法连接并配置基本FortiGate设置：
- 基于web的管理器
- 前面板控制键与LCD
- 命令行接口（CLI）

基于web的管理器

您可以通过任何运行微软Internet Explorer 6.0或其他最近版本的浏览器的计算机，使用HTTP或一个安全的HTTPS连接配置并管理FortiGate设备。基于web的管理器支持多种语言。
您可以使用基于web管理器配置大多数FortiGate设置并监控FortiGate设备的状态。

前面板控制键与LCD

您可以使用FortiGate设备前面板控制键与LCD配置IP地址以及默认网关与操作模式的切换。不用进入命令行接口或基于web的管理器，LCD可以显示设备运行的操作模式。有关面板控制键与LCD的详细信息，参见24页“LCD前面板控制键”。

命令行接口（CLI）

您可以通过连接到一个管理计算机串行端口进入FortiGate串行Console连接器，访问FortiGate命令行接口。您也可以从任何连接FortiGate设备的网络包括内部网，使用Telnet或一个安全的SSH连接接入到CLI。

连接到基于web的管理器

根据以下操作步骤建立与基于web管理器的初次链接。在基于web的管理器中所做的配置修改，无需重新设置防火墙或中断运行便可生效。

连接到基于web的管理器，您需要：
- 一台能够连接以太网的计算机
- 微软6.0版本的浏览器或以上的版本，或任何现行的web浏览器
- 一根交叉的以太网网线或一个以太网网络集线器（hub）与两根以太网网线。

注意：启动IE之前（或其他现行版本的的网页浏览器），ping FortiGate设备，检测计算机与FortiGate设备之间是否连接正常。

使用端口1连接到基于web管理程序

您可以使用端口1接口连接到基于web的管理器。没有光纤网络连接到内部接口时，FortiGate-3000的端口1接口可以作为可选接口。

使用端口1连接到基于web管理程序

1. 连接到FortiGate-3000命令行接口(CLI)。参见23页“连接到CLI”。
2. 把端口1的IP地址与掩码设置为您可以用计算机与以太网连接的地址，并设置到HTTPS的管理访问。

```
config system interface
  edit port 1
      set ip <address_ip> <netmask>
      set allowaccess https
  end
```

示例

设置端口1的IP地址为192.168.20.99，掩码为255.255.255.0并将管理访问设置为HTTPS，

输入：

```
config system interface
 edit port 1
    set ip <address_ip> <netmask>
    set allowaccess https
 end
```

3. 在同一个子网，设置计算机与以太网连接的IP地址为一个静态的IP。
4. 使用交叉线(或以太网网络集线器(hub)与网线)，建立FortiGate设备端口1到计算机以太网的连接。

使用内部接口连接到基于web的管理器

使用内部接口，FortiGate-3000可以连接到光纤网络，浏览基于web的管理器。

但是，FortiGate-3600需要执行以下的操作。

使用内部接口连接到基于web的管理器

1. 设置计算机与以太网连接的IP地址为静态IP地址192.168.1.2，掩码为255.255.255.0。
2. 将FortiGate设备的内部接口与您的光纤网络接口连接。
3. 将计算机的接口连接到同一网络中。
4. 启动IE浏览器，浏览地址为 https://192.168.1.99 的页面（请注意是https://）。

为了支持安全的HTTPS识别程序，FortiGate设备引入一个自签订的安全认证，每当远程用户对FortiGate设备发起一个HTTPS连接时，该安全认证便会弹出。当您进行连接时，FortiGate设备在浏览器中显示两个安全警告。

第一个警告信息提示您接受并安装FortiGate设备的自签安全证书。如

您不接收认证，FortiGate设备将拒绝连接。如您接收认证，将转入FortiGate登录页面。输入用户名与密码验证信息登录。如您选择永久接受认证，警告信息不再弹出。

在FortiGate登录页面显示之前，第二个警告信息告知您FortiGate认证与原始请求的区别。该信息弹出是因为FortiGate设备试图进行再次连接。是一条报告性信息。点击“OK”键确认，继续登录页。

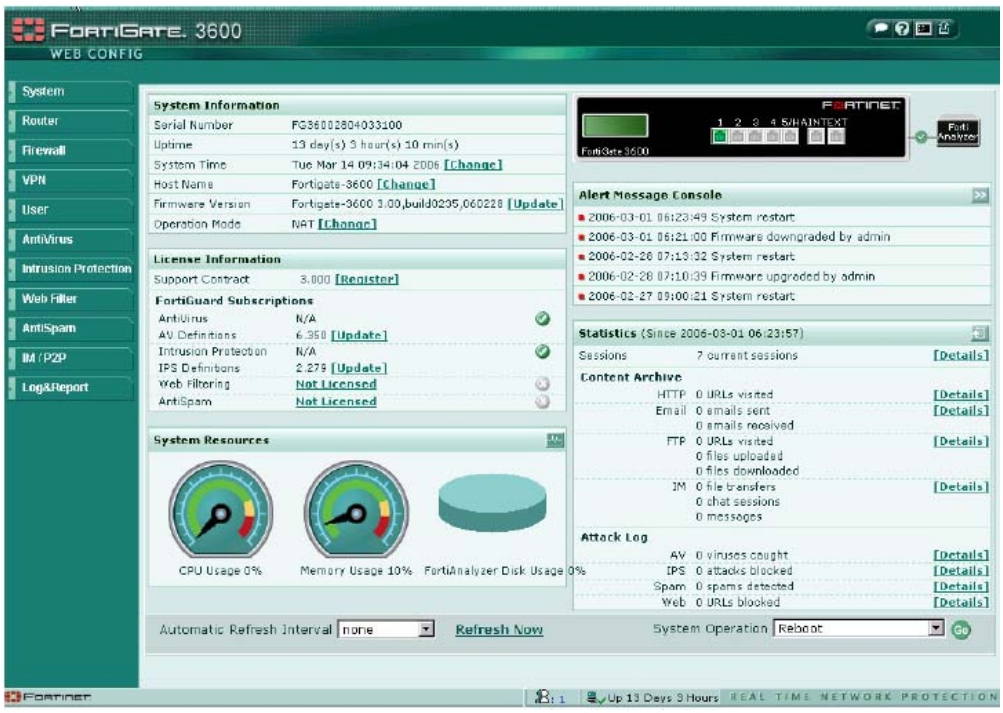
图3：FortiGate登录页面

5. 输入用户名与密码登录。

系统操作面板

登录到基于web的管理器后，页面显示系统操作面板。面板显示所有的系统状态信息。

图4：FortiGate-3000系统面板



面板中包括以下信息：

• 端口状态— 面板中显示有FortiGate设备的正面镜像图。包括FortiAnalyzer连接状态—X表示没有连接，当检测标志中没有标注X时，说明存在连接。滑动鼠标到每个端口，可以查看端口信息，如 IP地址与掩码，速率，以及接收或发送的数据包信息。当端口使用中时，其状态显示呈绿色。

• 系统信息— 操作系统信息的显示包括设备串行数量与固件版本。在该区域，可以进行固件升级，设置系统时间或更改操作模式。

• 系统资源— 显示系统资源使用情况。

• 许可证信息— 显示FortiGate设备中当前的病毒防护与安全性升级的情况。

• 报警信息Console — 显示最近FortiGate设备发出的警告日志信息。

• 统计表 — 提供FortiGate设备的实时流量与攻击信息。

连接到CLI（命令行接口）

除了使用基于web的管理器，您也可以使用CLI安装与配置FortiGate设备。无需重新设置防火墙或中断设备运行，CLI所进行的配置更改便可以生效。

• 一台有通信端口的计算机

• FortiGate设备包装中带有的交叉modem线

• 终端模拟软件，如Microsoft Windows的HyperTerminal。

连接到CLI

1. 使用交叉modem线将您计算机的通信端口与FortiGate console端口连接。

2. 启动HyperTerminal，键入连接的名称，点击OK确认。
3. 配置将HyperTerminal与您计算机的通信端口直接连接并点击OK键确认。
4.输入以下端口设置并点击OK确认。

Bit per second	9600
Bata bits	8
Partity	None
Stop bits	1
Flow control	None

5. 按Enter键，建立与FortiGate CLI的连接。
弹出登录页。
6. 键入admin的名称并按Enter键两次
显示如下提示信息;
Welcome!
键入？列出可用的命令。有关如何使用CLI（命令行接口）的详细信息，参见 *FortiGate CLI 参考手册*。

LCD前面板控制按键

您可以使用前面板控制按键与LCD对FortiGate设备进行基本的设置。该方法简单快捷。您可以配置：
- IP地址
- 掩码
- 默认网关
- 操作模式
- 恢复出厂默认设置

LCD所显示的是FortiGate设备的操作模式信息与该设备是否是HA（高可用性）群集的一部分。图5所示是FortiGate设备默认的LCD主菜单设置，NAT/路由器模式下不能与HA群集连接。

图5：默认LCD主菜单设置

表4：LCD主菜单定义

Manu	LCD现在所显示的菜单。
「FortiGate_>」	FortiGate 设备的主机名称。
NAT	FortiGate设备正在运行的操作模式。
Standalone	FortiGate设备不作为HA群集的一部分，有关Standalone（单机）模式与HA的详细信息，参见FortiGate设备管理员使用手册。

通过前面板控制按键，您可以进入与退出不同的菜单、配置不同的端口与接口。在配置IP地址、默认网关地址或是掩码时，前面板控制按键也可以增加或删减数值。下表是用于FortiGate设备的基本配置，按键的作用与功能。

表5：前面板控制按键定义

Enter	**前进键，移动进行配置菜单模块的选择**
ESC	**后退键，或从您所进入的菜单中退出**
UP	**IP地址、默认网关或子网掩码值的增加**
Down	**IP地址、默认网关或子网掩码值的删减**

前面板控制按键与LCD的使用

当LCD显示主菜单设置时，您便可以开始设置IP地址、掩码与默认网关；如需要，还可以更改操作模式。在33页中“在网络中配置FortiGate设备”时，以下操作可作为指导。

设置IP地址

按照以下步骤设置FortiGate设备的IP地址。

输入一个IP地址

1. 按Enter键选择端口。
2. 按UP与Down键加亮显示您所选择做IP地址设置的端口，然后按Enter键确认。
3. 按Enter键，进行IP设置。
4. 用UP与Down键增加或删减IP地址的数值。
5. Enter键选择数值。
6. 重复4与5完成IP地址的设置。

以上操作步骤同样适用于设置掩码与默认的网关。

更改操作模式

使用以下步骤更改FortiGate设备的操作模式。

更改操作模式

1. 确定LCD显示的是主菜单设置。
2. 按Enter键选择端口。
3. 用UP与Down加亮显示菜单“更改为桥接模式”。
4. 按Enter键更改为透明模式。

设备更改为透明模式。该更改过程需要几分钟时间实现。

5. LCD应该显示如图6所示：

图6：LCD主菜单设置的透明模式显示

恢复出厂默认设置

按照以下操作步骤，您可以恢复到FortiGate的出厂默认设置。有关恢复出厂设置的详细信息，参见31页 “恢复出厂默认设置”。

恢复为设置出厂设置的步骤

1. 确定LCD显示是主菜单设置
2. 按Enter键进入接口。
3. 按UP与Down键加亮显示菜单“恢复默认设置”。
4. 按Enter键确认。

FortiGate设备回复到出厂设置，该过程需要几分钟时间实现。

出厂默认设置

FortiGate设备有出厂默认设置。该默认设置允许您连接到FortiGate设备并能够使用FortiGate基于web的管理器在网络中配置FortiGate设备。在网络中配置FortiGate，您需要添加管理员密码，更改网络接口IP地址与DNS服务器的IP地址，如有必要，可以配置基本的路由。

如果您打算以透明模式运行FortiGate设备，可以从出厂默认配置中切换到透明模式，并根据您的网络结构与情况配置透明模式下的FortiGate设备。

完成网络配置后，您还可以进行其他的配置操作，如设置系统时间，配置病毒及攻击的定义更新，注册FortiGate设备等。

出厂时默认的防火墙配置包括单一网络地址转换（NAT）策略，该策略允许您内部网络的用户连接到外部网络，同时阻止外部网络中的用户连接到内部网络。您可以添加更多其它的策略，对通过FortiGate 设备的流量进行更多的控制。

出厂时默认的内容配置文件可以用来快速地在防火墙策略中设置不同级别的防病毒保护、网页内容过滤、垃圾邮件过滤，以便控制网络通讯。

本章包括以下内容：

- 出厂默认的防火墙保护内容设置
- 恢复默认配置

出厂默认的NAT/ 路由模式的网络配置

FortiGate设备首次启动时，它运行于NAT/路由模式，表2所列是该工作模式下的基本网络配置。该配置允许您连接到FortiGate设备的基于web的管理器，并建立FortiGate设备连接到网络所需的配置。28页中表6中，HTTPS管理访问表示您可以通过该接口的HTTPS协议连接到基于web的管理器。Ping管理访问表示该接口对ping这一命令可以做出响应。

表6：出厂默认的NAT/路由模式的网络配置

管理员账号	用户名： 密码：	Admin （无）
内部接口	IP： 子网掩码： 管理访问：	192.168.1.99 255.255.255.0 HTTPS，Ping
外部接口	IP： 子网掩码： 管理访问：	192.168.100.99 255.255.255.0 Ping
端口1	IP： 子网掩码： 管理访问：	0.0.0.0. 0.0.0.0. Ping
端口2	IP： 子网掩码： 管理访问：	0.0.0.0. 0.0.0.0. Ping
端口3	IP： 子网掩码： 管理访问：	0.0.0.0. 0.0.0.0. Ping
端口4	IP： 子网掩码： 管理访问：	0.0.0.0. 0.0.0.0. Ping
端口4/HA 与端口5/HA	IP： 子网掩码： 管理访问：	0.0.0.0. 0.0.0.0. Ping
网络设置	默认网关（默认路由）	192.168.100.1
	连接到外部网络的接口（默认路由）	外部
	默认路由 默认的路由由一个默认的网关与连接到外部网络（通常是互联网）接口的名称组成。 默认的网关将所有非本地的通讯集中到该接口与外部网络。	
	一级DNS：	65.39.139.53
	二级DNS：	65.39.139.63

出厂默认的透明模式的网络配置

29页表7是透明模式下，FortiGate设备默认的网络配置。

表7：出厂默认的透明模式网络配置

管理员帐户	用户名： 密码：	Admin （无）
管理IP	IP： 子网掩码：	0.0.0.0. 0.0.0.0.
DNS	一级DNS服务器 二级DNS服务器	65.39.139.53 65.39.139.63
管理访问	内部 外部 端口1 端口2 端口3 端口4 端口4/HA 端口5/HA	HTTPS，ping Ping Ping Ping Ping Ping Ping Ping

出厂默认防火墙设置

FortiGate防火墙策略是有关FortiGate设备对所有通讯流量的控制。除非添加了防火墙策略，否则没有流量通讯能够被FortiGate设备接收或经过FortiGate设备。您可以添加防火墙策略允许网络流量通过FortiGate设备。有关添加防火墙策略，参见*FortiGate管理员使用手册*。

以下是默认的防火墙配置中的策略配置设置：

表8：出厂默认防火墙配置

配置设置	名称	描述
防火墙地址	所有	防火墙地址与任何数据包的源目标地址匹配。
预先定义的服务	50多条预先定义的服务	从50多条预先定义的服务中选择控制通过FortiGate流量的服务。
循环任务时间表	总是	任何时间，循环任务计划都是有效的。
防火墙保护	Stict,Scan,Web,Unfiltered	控制防火墙设备是怎样启用病毒扫描，网页内容过滤，垃圾邮件过滤与IPS。

NAT/路由模式与透明模式下防火墙配置的出厂默认设置是相同的。

出厂默认的防火墙保护内容设置

使用防火墙保护设置对防火墙策略控制的流量进行不同的防护设置。

- 给HTTP，FTP，IMAP，POP3与SMTP防火墙策略配置防病毒保护。
- 给HTTP防火墙策略配置网页过滤。
- 给HTTP策略配置网页类别过滤。
- 给IMAP， POP3与SMTP防火墙策略配置垃圾邮件过滤。
- 对所有的服务启动入侵防护系统（IPS）。
- 对HTTP，FTP，IMAP，POP3与SMTP防火墙策略启动内容日志

通过防火墙保护，您可以构建适用与不同类型防火墙策略的保护配置。并允许您针对不同防火墙策略定制不同类型与级别的防护。

例如，内部与外部地址之间的流量可能需要比较严格的防护，而内部地址之间的流量可能需要中等一般的防护。您可以针对不同的流量使用相同或不同的保护设置配置防火墙策略。

NAT/路由模式与透明模式的防火墙策略也可以添加保护设置。

FortiGate设备可以预先配置四种保护设置。

Strict（严格型） 适用于对HTTP，FTP， IMAP，POP3与SMTP流量应用最大限度的保护。一般情况下，不必使用Strict（严格型）的保护设置，发现病毒攻击，需要扫描检测时，可以启用Strict（严格型）保护。

Scan （扫描型） 针对HTTP，FTP，IMAP，POP3，与SMTP内容流量采用病毒扫描与文件隔离。

Web （网页内容控制型） 针对HTTP内容流量采取病毒扫描与网页内容屏蔽。您可以在防火墙策略中添加该保护设置来控制HTTP流量。

Unfiltered （无过滤型） 如果对于内容流量不愿意采用内容防护，您可以使用无过滤型保护。您可以在不需要内容保护的高可信与安全性较高的网络连接区域，在防火墙的策略中添加该保护设置。

恢复出厂默认设置

如果您误更改了网络设置，并无法恢复，您可以先恢复到出厂默认设置然后重新启动。

 该操作将删除您对FortiGate做的所有配置更改，并将系统退回至原始配置包括重新设置接口地址。

使用基于web的管理器恢复默认的出厂设置

恢复默认的设置

1. 进入**系统>系统状态>系统操作。**
2. 点击“恢复为出厂默认设置”。
3. 点击“确认”。

使用CLI恢复默认的出厂设置

键入如下命令恢复为出厂默认设置：

```
execute factoryreset
```

 **注意：**如果您想使用前面板控制按键与LCD恢复出厂默认设置，参见24页“前面板控制按键与LCD”。

在网络中配置FortiGate设备

本章是FortiGate设备的操作模式说明。开始配置FortiGate设备之前，先要考虑怎样将FortiGate设备集成到网络中。 针对不同的操作模式，NAT/路由模式或透明模式，进行对应的配置。

该章节包括以下内容：

规划FortiGate配置

配置FortiGate设备之前，先要考虑怎样把FortiGate设备集成在网络中。至于其它问题，如还需要决定FortiGate设备是否在网络中可见，需要配置哪些防火墙功能，与怎样控制接口间的流量。

您所选择的FortiGate设备的操作模式是配置的依据。FortiGate设备有两个模式，分别为：NAT/路由模式（出厂默认）与透明模式。

您也可以在出厂默认的操作模式设置即NAT/路由模式下，在网络中配置FortiGate设备。

NAT/路由模式安装

NA/路由模式下，FortiGate设备在网络中是可见的类似一个路由器，设备的所有接口在不同的子网中。在NA/路由模式下，以下接口是可用的。

表9：NAT/路由模式下的网段

FortiGate设备	内部接口	外部接口	其他
FortiGate-3000	Internal	External	Port2 Port1，3，4 Port 4/HA
FortiGate-3600	Internal	External	Port1 Port2，3，4 Port 5/HA

您可以添加防火墙策略控制NAT/路由模式下的FortiGate设备是否有通信流量通过。防火墙策略根据源地址、目标地址与每个数据包的服务来控制数据流量。 NAT模式下，FortiGate设备发送数据包到目标网络之前，先执行网络地址转换。路由模式操作没有地址转换。

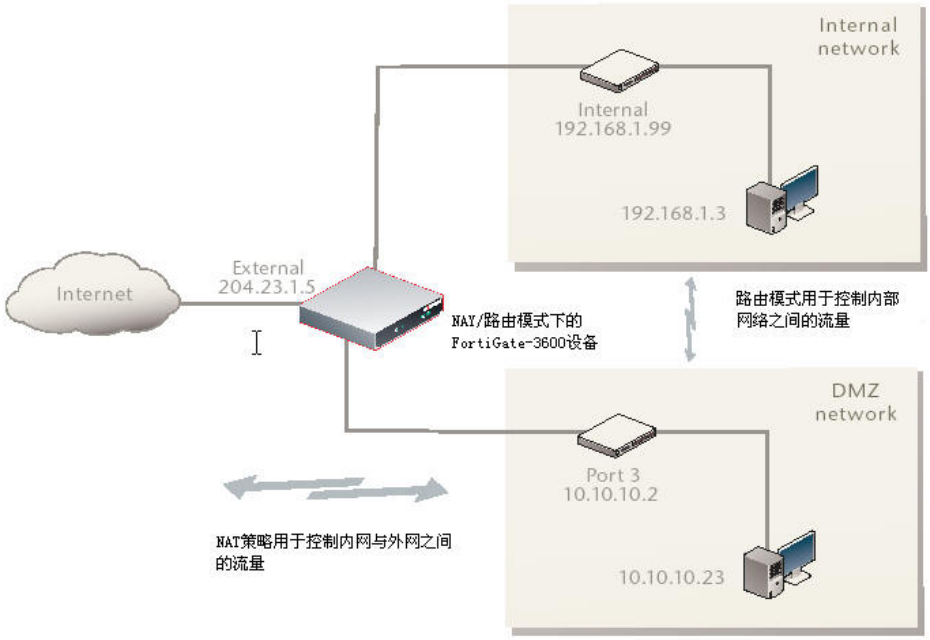
NAT/路由模式下的FortiGate设备的典型的应用是作为私网与公网之

间的网关。该配置中，您可以建立NAT模式防火墙策略控制内部网、私网与外部网，公网（通常指互联网）之间的数据流量。

注意：如果是多重内部网络连接，例如内部网之外的DMZ网络、私网；您可以建立路由模式下的防火墙策略控制这些多重网络之间的流量。

.

图7：FortiGate-3600 NAT/路由模式下的网络配置举例



具有多个外部网络连接的NAT/路由模式

NAT/路由模式下，您可以配置FortiGate设备具有多个冗余连接，连接到外部网络（通常指互联网）。

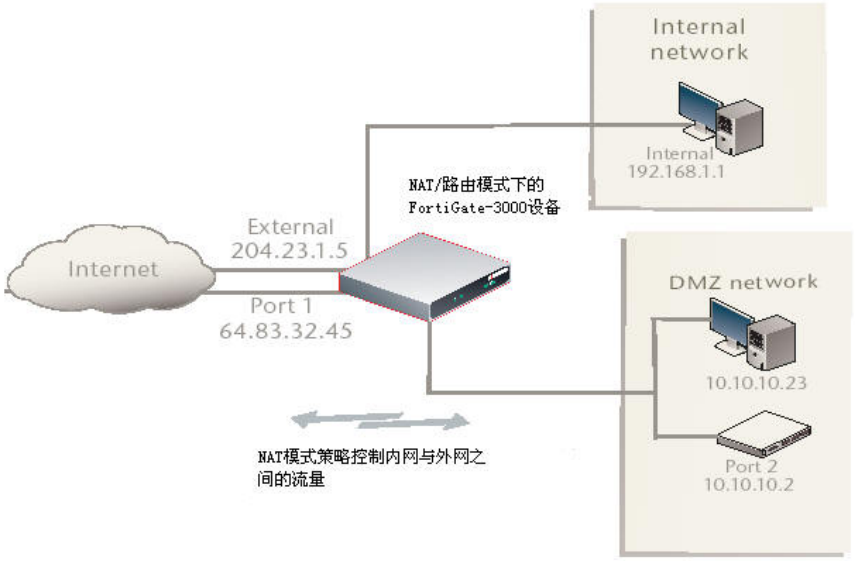
例如，您可以创建以下配置：

- External（外部）指连接到外部网络（通常指互联网）的默认接口。
- Internal（内部）指连接到内部网络的接口。
- Port 1 （端口1）是连接到外部网络的冗余接口。
- Port 2 （端口2）是连接到DMZ网络的接口。

您需要配置路由以支持冗余的Internet（互联网）连接。如果连接外部网络失败，路由可以自动从接口选择，重新定向连接。

或者，安全策略配置类似一个具有单向互联网（Internet）连接的NAT/路由模式。您可以创建NAT模式防火墙策略控制内部网、私网与外部网，公网（通常指互联网）之间的流量。

图8：FortiGate-3000设备NAT/路由模式下多重internet（互联网）连接配置举例



透明模式

透明模式下，FortiGate设备在网络中是透明的。类似于网络桥梁，所有的FortiGate接口都在同一个子网中。您只需配置一个管理IP地址便可以进行配置更改。管理IP地址也可用来配置病毒及攻击的定义更新。透明模式下的FortiGate设备的典型应用位于当前的防火墙或路由器之后。FortiGate设备具有防火墙，IPsec，病毒扫描，IPS 网页过滤与垃圾邮件过滤功能。

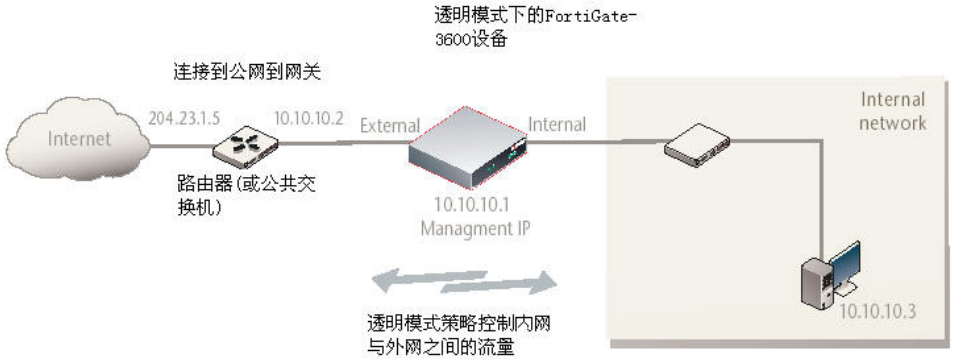
您最多可以将6个网段连接到FortiGate设备上，以控制这些网段之间的数据流量。

表10：透明模式下的网络分段

FortiGate设备	内部接口	外部接口	其他
FortiGate-3000	Internal	External	Port 1 到 Port 4/HA
FortiGate-3600	Internal	External	Port1 到 Port 5/HA

注意：当您安装HA群集时，端口4/HA用于连接到其它FortiGate-3000备，端口5/HA用于连接到其它FortiGate-3600。

图9：FortiGate-3600设备透明模式下的网络配置举例



设置公共FortiGate接口对Ping命令请求不作出响应

出厂默认的FortiGate设备允许默认的公共接口对ping请求作出响应。默认的工作接口也称为默认的外部接口，该接口是通常用于连接到互联网的接口。

出于安全操作着想，您应该更改外部接口的配置，对外部的ping请求不作出响应。配置对外部的ping请求不作出响应增强了网络的安全性，增加网络中可能的攻击对FortiGate设备的探测。

FortiGate-3000与FortiGate-3600设备默认的公共接口是它的外部接口。

如果对接口启动了ping管理访问设置，那么FortiGate设备将对ping请求作出响应。您可以使用以下操作步骤撤消对FortiGate设备外部接口的ping访问。同样的操作适用于任何操作模式下的设备接口。

使用基于web的管理器撤消ping管理访问

1. 登录基于web的管理器。
2. 进入系统>网络设置〉接口。
3. 选择外部接口并点击对应的“编辑”。
4. 撤消Ping 管理访问功能。
5. 点击OK保存该配置更改。

使用CLI撤消ping管理访问

1. 登录FortiGate CLI。
2. 输入以下命令，撤消对外部接口的管理访问：

```
config system interface
  edit external
    unset allowaccess
end
```

NAT/路由模式安装

本章介绍了如何在NAT/路由模式下安装Fortigate设备。包括以下内容：

- 配置DHCP或PPPoE
- 使用基于web的管理器
- 使用前面板控制按键与LCD
- 使用命令行接口（CLI）
- 将FortiGate设备配置到网络中
- 配置网络

配置FortiGate设备的NAT/路由模式准备

参考37页表9中的信息，您可以定制NAT/路由模式设置。

您可以使用以下几种方法配置FortiGate设备：

- 通过基于web的管理器的用户界面可以配置设备的大部分设置。参见38页“使用基于web的管理器”。
- 通过前面板控制按键与LCD可以配置IP地址，默认网关与操作模式。参见39页“使用前面板控制按键与LCD”。
- 使用命令行接口（CLI）可以配置设备的全部设置。参见40页“使用命令行接口（CLI）”。

根据配置，访问与设备组合的复杂性与您惯用的接口类型选择合适的配置方法。

表11：NAT/路由模式设置

管理员密码		
内部	**IP：** **子网掩码：**	_____ • _____ • _____ _____ • _____ • _____
外部	**IP：** **子网掩码**	_____ • _____ • _____ _____ • _____ • _____
端口1	**IP：** **子网掩码**	_____ • _____ • _____ _____ • _____ • _____
端口2	**IP：** **子网掩码**	_____ • _____ • _____ _____ • _____ • _____
端口3	**IP：** **子网掩码**	_____ • _____ • _____ _____ • _____ • _____
端口4	**IP：** **子网掩码**	_____ • _____ • _____ _____ • _____ • _____
端口4/HA	**IP：** **子网掩码**	_____ • _____ • _____ _____ • _____ • _____
端口5/HA	**IP：** **子网掩码**	_____ • _____ • _____ _____ • _____ • _____
网络设置	**默认网关：** **（与外部网络连接的接口）**	_____ • _____ • _____

	默认路由由默认的网关与连接到外部网络（通常指互联网）的接口组成。默认的网关将所有非本地流量集中到该接口与外部网络中。	
	一级DNS服务器： 二级DNS服务器：	_____ • _____ • _____ _____ • _____ • _____

配置使用DHCP或PPPoE

您可以配置任何FortiGate接口从DHCP或PPPoE服务器获得IP地址。您的互联网服务提供商（ISP）便是使用这其中的一项协议提供IP地址的。

使用FortiGate DHCP服务器，您需要配置该服务器的IP地址范围与默认的路由。将接口配置为使用DHCP便不需要做更多的配置了。

配置使用PPPoE需要设置用户名与密码。另外，PPPoE未编号配置要求固定一个IP地址。参考表10记录的信息配置PPPoE。

表10：PPPoE设置

用户名	
密码	

使用基于web的管理器

您可以使用基于web的管理器进行FortiGate设备的初始配置以及所有FortiGate设备的设置。

有关连接到基于web的管理器信息，参见20页“连接到基于web的管理器”。

配置基本设置

连接到基于web的管理器后，您可以使用以下操作完成FortiGate设备的基本配置。

添加或更改管理员密码

1. 进入**系统> 管理员配置> 管理员。**
2. 点击“更改密码”图标更改管理员密码。
3. 输入新密码，再输入一次确认。
4. 点击OK确认。

配置接口

1. 进入**系统> 管理员配置> 管理员。**
2.点击接口的“编辑”图标。
3.设置接口的地址模式。
从菜单中选择DHCP或PPPoE.
4.完成地址配置。
• 对于手动的地址，输入接口的IP地址与掩码
• 对于DHCP地址，点击DHCP并进行任何需要的设置
• 对于PPPoE地址，点击PPPoE后输入用户名与密码
有关接口设置的配置，参见FortiGate在线帮助或*FortiGate设备管理员使用手册。*
6. 点击“OK”确认
重复以上步骤，对每个接口进行配置。

注意：如果您想更改连接接口的IP地址，您必须使用新的地址通过网页浏览器重新连接。浏览http：//后跟接口新的IP地址。如果接口新的IP地址是不同的子网，您还需将计算机IP地址更改为与该子网相同的IP地址。

配置DNS服务器设置

1.进入**系统>网络配置>选项。**
2.输入一级DNS服务器的IP地址。
3.输入二级DNS服务器的IP地址。
4.点击“应用”。

添加默认路由

FortiGate设备发送数据包到外部网络（通常指互联网）时，需要配置添加默认的路由。添加默认的路由也需要定义哪个接口连接到外部网络。如果与外部网络连接的接口配置使用了DHCP或PPPoE，则不需要添加默认的路由。

添加默认路由

1.进入**路由>静态路由**。
2.如果静态路由表格中有默认的路由设置（IP与掩码设置为0.0.0.0.），点击“删除”图标删除该路由。
3.点击“新建”。
4.设置目标IP地址为0.0.0.0.
5.设置掩码为0.0.0.0.
6.设置网关为默认的网关IP地址
7.设置连接到外部网络接口的驱动。
8.点击OK确认。

校验基于web管理器配置

校验访问设置，进入所校验的接口并点击编辑图标。管理访问字段有检验标识可以确认是否执行了校验。

校验连接

使用以下步骤校验连接：

- 访问www.fortinet.com
- 从您的邮件帐户收发电子邮件

如果您不能浏览fortinet网站或收发电子邮件，请检查以上步骤确保所输入的信息正确，再试一次。

使用前面板控制按键与LCD

基本设置，包括接口IP地址、掩码、默认网关与FortiGate操作模式均可使用前面板控制按键与LCD进行配置。参考37页表9中所记录的信息完成以下步骤。LCD显示主菜单时，便可以开始设置。使用控制按键与LCD配置接口时，接口的名称通常显示为internal（内部），External（外部）与DMZ。LCD所显示的接口名称与以下FortiGate设备接口名称相对应。

表13：FortiGate设备接口

控制按键与LCD接口名称	FortiGate设备接口名称
Internal Port（内部端口）	Internal（内部）
External Port（外部端口）	External（外部）
DMZ Port（DMZ端口）	3

更改接口的IP地址与掩码

1. 按Enter键显示接口列表。
2. 使用上下方向方向键选择要更改的接口后按Enter。
3. 按Enter键显示IP地址。
4. 使用上下方向键添加或删减每个IP地址的数值。按Enter键移动到下一个数值。Esc键可以回退到前一位数值。
5. 设置了全部IP地址数值后，按Enter键。
6. 使用下方向键选择掩码。
7. 按Enter键进行掩码更改。
8. 设置完全部掩码数值后，按Enter键。

按Esc返回主菜单设置。

使用LCD添加默认网关

通常对与互联网连接的接口配置网关。您可以使用以下步骤对任何接

口配置默认的网关。

给接口添加默认的网关

1. 按Enter键显示接口列表
2. 使用下方向键加亮显示与互联网连接的接口，按Enter键。
3. 使用下方向键选择默认网关。
4. 按Enter键，设置默认网关
5. 设置了全部默认网关数值后，按Enter键。
6. 按Ese返回主菜单设置。

只能使用基于web的管理器或CLI配置DNS服务器设置。LCD中没有配置DNS服务器设置的选项。

校验前面板控制按键与LCD配置

校验访问设置，进入所要校验的接口并点击编辑图标。管理访问字段有检验标识可以确认是否是否执行了校验。

校验连接

使用以下步骤校验连接：

- 访问www.fortinet.com
- 从您的邮件帐户收发电子邮件

如果您不能浏览fortinet网站或从您的帐户收发电子邮件，请检查以上步骤确保所输入的信息正确，再试一次。

使用命令行接口（CLI）

您可以使用命令行接口（CLI）对FortiGate设备进行配置。有关连接到CLI的详细信息，参见23页“连接到CLI”。

配置FortiGate设备运行于NAT/路由模式

参考37页表格9中所采集的信息完成以下步骤。

添加或更改管理员命令

1. 登录到CLI（命令行接口）
2. 更改管理员密码。输入：

```
config system admin
  edit admin
    set password <psswrd>
  end
```

配置接口

1. 登录到CLI（命令行接口）

2. 设置内部接口的IP地址与掩码为37页表格9中所记录的内部IP地址与掩码。输入：

```
config system interface
    edit internal
        set mode static
        set ip <address_ip> <netmask>
    end
```

举例

```
config system interface
  edit internal
    set mode static
    set ip 192.168.120.99 255.255.255.0
end
```

3. 设置外部接口的IP地址与掩码为37页表格9中所记录的外部IP地址与掩码。输入：

```
config system external
    edit external
        set mode static
        set ip <address_ip> <netmask>
    end
```

举例

```
config system external
    edit external
      set mode static
      set ip 204.28.1.5 255.255.255.0
end
```

设置外部接口使用DHCP

```
config system interface
  edit external
    set mode dhcp
end
```

设置外部接口使用PPPoE

```
config system interface
  edit external
    set mode pppoe
    set connection enable
    set username <name_str>
    set password <psswrd>
end
```

4. 根据需要使用命令句法模式配置每个接口的IP地址。

5. 确认输入的地址是正确的。输入：

```
get system interface
```

CLI命令行接口列出了每个FortiGate接口的IP地址、掩码、与其他设

置。

配置DNS服务器设置

设置一级与二级DNS服务器的IP地址。输入：

```
config system dns
    set primary <address_ip>
    set secondary <address_ip>
  end
```

举例

```
config system dns
    set primary 293.44.75.21
    set secondary 293.44.75.22
  end
```

添加默认的路由

FortiGate设备发送数据包到外部网络（通常指互联网）时，需要配置添加默认的路由。添加默认的路由也需要定义哪个接口连接到外部网络。如果与外部网络连接的接口配置使用了DHCP或PPPoE，则不需要默认的路由。

添加默认的路由

设置默认网关IP地址的路由。输入：

```
config router static
  edit 1
      set dst 0.0.0.0 0.0.0.0
      set gateway <gateway_IP>
      set device <interface>
  end
```

举例

如果默认的网关IP地址是204.23.1.2，该网关连接到端口1：

```
config router static
  edit 1
      set dst 0.0.0.0 0.0.0.0
      set gateway 204.23.1.2
      set device port1
  end
```

校验CLI配置

输入以下CLI命令校验访问设置：

```
show system interface
```

终端模拟程序（Terminal emulation program）显示接口、vdom、IP地址、允许访问与FortiGate设备的类型设置；如以下例子所示：

```
edit internal
  set vdom “root”
  set ip 192.168.1.99 255.255.255.0
  set allowaccess ping https ssh snmp http
  set type physical
```

校验连接

使用以下步骤校验连接：

- ping FortiGate设备
- 查看基于web管理程序的图形用户界面
- 使用您的邮件帐户收发电子邮件

如果您不能登录基于web管理程序或收发电子邮件，请检查以上步骤确定所输入的信息正确，再试一次。

至此，FortiGate设备的初始化配置完成。

将FortiGate设备连接到网络中

当您完成Fortigate设备的初始化配置后，便可以在您的内部网与互联网之间连接FortiGate设备了。

以下是FortiGate设备中可用的网络连接：

- Internal可以连接到您的内部网络。
- External可以连接到互联网。
- 接口3可以连接到DMZ网络。

与FortiGate设备建立连接：

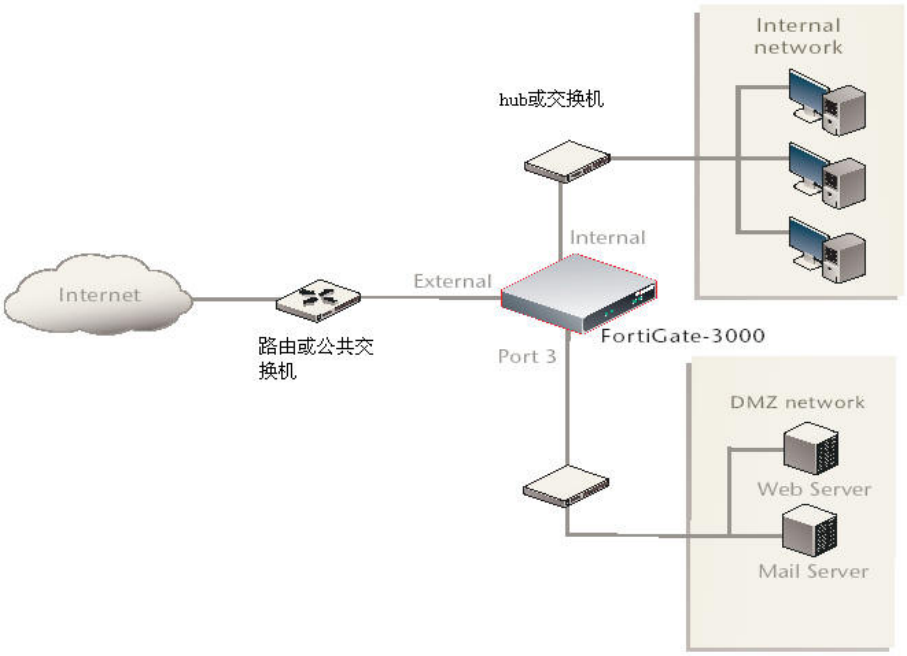
1.通过将内部接口连接到hub或交换机，接入内部网络。

2.将外部接口（External）与互联网连接。连接到ISP服务商提供的公共交换机或路由器。如果您是DSL或有线网络用户，将外部接口与内部网络或您DSL的LAN连接或有线调制解调器连接。

3.接口3是连接DMZ网络的可选接口。

通过DMZ网络，无需在您的内部网络安装服务器，便可以进行从互联网到网络服务器或其他服务器的访问。

图10：FortiGate-3000 NAT/路由模式连接



配置网络

如果FortiGate设备运行于NAT/路由模式，您需要给网络配置路由，使所有的网络流量都能够流向与网络连接的接口。
- 对于内部网络，更改与内部网络直接连接的所有计算机与路由器默认的网关地址为FortiGate内部接口的IP地址。
- 对于外部网络，路由所有数据包到FortiGate外部接口。
- 对于DMZ网络，更改与您的DMZ网络直接连接的所有计算机与路由器默认的网关地址为FortiGate设备DMZ接口的IP地址。

如果您将FortiGate设备作为内部网络中的DHCP服务器使用，需要配置内部网络的计算机使用DHCP。

通过内部网络的计算机连接到互联网，确定连接的FortiGate设备工作正常。您应该可以连接到任何互联网地址。

透明模式安装

本章介绍了如何安装透明模式下安装FortiGate设备。包括以下内容：
- 配置透明模式的准备
- 使用基于web管理程序
- 使用前面板控制按键与LCD
- 使用命令行接口(CLI)
- 将FortiGate设备连接到网络中

根据配置、访问与设备的复杂程度，选择以上所列出的方法。

配置透明模式的准备

参考表14的信息定制透明模式设置。

以下三种方法均可配置透明模式：
- 基于web管理程序的GUI
- 前面板控制按键与LCD
- 命令行接口（CLI）

根据配置，访问与设备的复杂性与您惯用的接口类型选择配置透明模式的方法。

表14：透明模式设置

管理员密码：		
管理IP	**IP：** **掩码：** **默认网关：**	_____ • _____ • _____ • _____ _____ • _____ • _____ • _____ _____ • _____ • _____ • _____
	管理IP地址与掩码对于您所管理的FortiGate设备来讲必须是有效的网络地址。如果FortiGate设备需要连接到路由器后才能到达管理计算机，那么需要添加默认的网关。	
DNS设置	**一级DNS服务器：** **二级DNS服务器：**	_____ • _____ • _____ • _____ _____ • _____ • _____ • _____

使用基于web的管理器

您可以使用基于web的管理器完成FortiGate设备初始化配置以及设置功能选项。

有关连接到基于web的管理器信息，参见20页“连接到基于web管理程序”。初次连接到FortiGate设备时，默认操作模式是NAT/路由模式。

使用基于 web 的管理器切换到透明模式

1. 进入**系统>系统状态。**
2. 点击“操作模式”选项旁边的的“更改”。
3. 在操作模式列表中选择透明（Transparent）模式。
输入46页表14中收集的管理IP/掩码地址与默认网关地址。
4. 点击应用。

无需与基于web的管理器重建建立连接。点击应用后，配置更改即可生效，您可以进入系统面板对更改为透明模式下的FortiGate设备进行校验。

配置DNS服务器设置

1. 进入**系统>网络设置>选项。**
2. 输入一级DNS服务器的IP地址
3. 输入二级DNS服务器的IP地址
4. 点击应用。

使用前面板控制按键与LCD

以下操作是关于如何使用控制按键与LCD配置透明模式的IP地址。46页表12所记录的信息可以协助完成该操作。LCD显示主菜单设置时，便可以开始以下操作。

注意：您也可以使用LCD与前控制按键切换到透明模式。详细信息，参见24页“LCD前面板控制按键”说明。

更改管理IP地址与掩码

1. 持续按Ese键直至出现主菜单设置（4秒后）。
2. 连续按Enter键三次进行管理接口IP地址配置。
3. 设置管理接口IP地址。
使用上下方向增加或删减每位IP地址的数值。Enter移动到下一位数值，Ese返回上一位数值。
4. 设置完IP地址后，按Enter键。
5. 使用下方向键移动到掩码并加亮显示。
6. 按Enter键并更改管理IP掩码
7. 设置完掩码后，按Enter键确认。
8. 按Esc返回主菜单设置
9. 如需要，重复以上步骤配置默认网关。

使用LCD添加默认网关

与互联网连接的接口一般需要配置默认网关。您可以使用以下操作给任何的接口配置默认的网关。

给接口添加默认的网关

1. 按Enter键显示接口列表。
2. 使用下方向键加亮显示与互联网连接的接口并按Enter键。
3. 使用下方向键加亮显示“默认网关”。
4. 按Enter键，设置默认的网关。
5. 设置完默认的网关后，按Enter键确认。
6. 按Ese返回主菜单设置。

您只能通过基于web管理程序或CLI配置DNS服务器的设置。LCD中没有配置DNS服务器设置的选项。

校验前面板控制按键与LCD配置

校验通过前面板控制按键与LCD配置的接口设置，访问基于web的管理器，进入**系统>网络设置>接口**。显示通过前面板控制按键与LCD配置的接口IP地址。

校验连接

使用以下步骤校验连接：

- 访问www.fortinet.com
- 从您的邮件帐户收发电子邮件

如果您不能浏览fortinet网站或从您的帐户收发电子邮件，请检查以上步骤确保所输入的信息正确，再试一次。

使用命令行接口（CLI）

除了使用基于web的管理器，您也可以使用命令行接口（CLI）对FortiGate设备进行初始化配置，参见23页“连接到命令行接口（CLI）”说明。46页表2中的收集的信息，可以协助完成以下操作。

使用CLI更改为透明模式

1. 登录到CLI
2. 切换到透明模式。输入：

```
config system settings
    set opmode transparent
    set manageip <address_ip> <netmask>
    set gateway <address_gateway>
  end
```

几秒后，显示以下信息：

```
Changing to TP mode
```

3. 登录页弹出时，输入以下命令：

```
get system settings
```

CLI显示FortiGate设备的状态包括管理IP地址与掩码：

```
opmode : transparent
manageip : <address_ip><netmask>
```

您需要校验DNS服务器设置的正确性。DNS设置是沿用NAT/路由模式的，对于透明模式可能并不正确。使用46页表12信息配置DNS服务器设置。

校验DNS服务器设置

输入以下命令检验FortiGate设备的DNS服务器设置：

```
show system dns
```

键入上述CLI命令后显示如下DNS服务器设置信息：

```
config system dns
    set primary 293.44.75.21
    set secondary 293.44.75.22
    set fwdintf internal
  end
```

配置DNS服务器设置

设置一级与二级DNS服务器IP地址。输入命令：

```
config system dns
  set primary <address_ip>
```

```
  set secondary <address_ip>
end
```

重新连接到基于web的管理器

当FortiGate设备切换到透明模式后,您可以使用新的IP地址重新连接到基于web的管理器。键入HTTP：//加新的IP地址。如果您通过一个路由器连接到管理接口，请确认是否在管理IP默认的网关字段添加了路由连接的网关。

将FortiGate设备连接到网络

完成设备初始化配置,便可以将FortiGate连接到您的内部网络与互联网之间，或是通过DMZ接口连接到其它网络中。

与透明模式运行下的FortiGate设备连接

1. 与连接到您内部网络的网络集线器（hub）或交换机通过内部接口建立连接。
2. 与连接到外部防火墙或路由器的网段建立连接。
3. 接口3连接到其它网络。

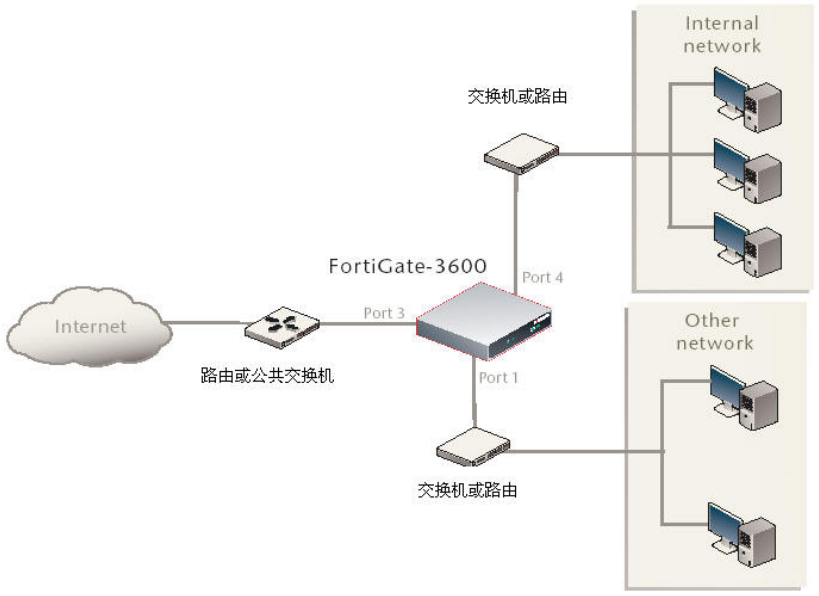
校验连接

使用以下操作校验连接：

- Ping FortiGate设备
- 登录到基于web的管理器
- 从您的邮件帐户收发电子邮件

如果您不能够正常浏览网站或收发电子邮件，检查以上步骤确定输入的信息正确，然后再试一次。

图11：FortiGate-3600透明模式连接



下一步

以下是关于配置FortiGate系统时间，FortiGate设备注册，以及配置病毒与攻击定义的更新的内容说明。
参见*FortiGate管理员使用手册*有关FortiGate设备的配置，监控与维护信息。

设置系统日期与时间

为了便于部署与记录日志，需要准确设置FortiGate设备的系统时间与日期。您可以手动设置系统时间与日期，或通过与网络时间协议（NTP）服务器同步自动校准时间。

设置日期与时间

1. 进入**系统>系统状态**。
2. **系统信息>系统时间**菜单选项下，点击“更改”。
3. 点击“刷新”显示当前的FortiGate系统日期与时间。
4. 从时区（Time Zone）列表中选择时区。
5. 可选择“自动”选项自动调整夏令时。
6. 点击“设置时间”，设置FortiGate系统日期与时间。
7. 设置时，分，秒，月，日，年。
8. 点击OK确认。

注意：如果您选择了根据夏令时自动调整时间，系统的时间必须在夏令时结束后手动重新调整。

使用NTP设置FortiGate设备的日期与时间

1. 进入**系统管理>系统状态**。
2. **系统信息> 系统时间**选项下，点击更改。
3. 选择“与NTP服务器保持同步”，配置FortiGate使用NTP自动设置系统时间与日期。
4. 输入NTP服务器的IP地址与域名，便于FortiGate设备自动设置时间与日期。
5. 注明FortiGate设备与NTP服务保持时间日期同步校准的频率。
6. 点击OK确认

FortiGate设备注册

FortiGate设备安装完成后，访问http://support.fortinet.com并点击“产品注册”进行设备注册。

输入您的联系方式与所购买的FortiGate设备序列号进行注册。您可以在注册栏中对所购买的全部设备进行同时注册，而无需重复输入联系信息。

通过FortiGate设备注册，您将接收到Fortinet公司发布的病毒与入侵检测等的更新并确保您能够访问Fortinet技术支持。

更新病毒防护与IPS特征

您可以配置FortiGate设备连接到FortiGuard Distribution Network进行病毒防护升级，反垃圾邮件与IPS攻击的定义更新。

FDN是遍及全世界范围的FDS服务器网络。 当FortiGate设备连接到FDN，根据就近原则，所有的FortiGate设备根据设备配置中的时区中相隔位于最近时区的FDN进行划分。

通过基于web的管理器或CLI，您可以更新病毒保护与IPS特征。设备在接收更新之前，需要先登录Fortinet网站进行注册。有关FortiGate设备注册的详细信息，参见50页“FortiGate设备注册”。

FortiGate设备注册后，校验是否能够与FDN连接：
- 检查FortiGate设备的系统时间是否正确。
- 登录基于web管理程序，在FortiGuard Center选项中点击“刷新”。

如果您不能连接到FDN，检查注册FortiGate设备步骤是否正确后，再试一次连接；或参见53页“添加替代的FDN服务器”。

使用基于web的管理器更新病毒防护与IPS特征

FortiGate设备注册完成后，您可以使用基于web的管理器更新病毒防护与IPS特征。FortiGuard 中心将发送推进式更新，您需要设置接收更新的IP地址，以及指定更新的时间频率如每日、每周或隔小时。

更新病毒防护定义与IPS特征

1. 进入**系统管理>系统维护> FortiGuard中心**.
2. 点击“立即更新”，进行病毒防护更新。

如果与FDN连接良好，基于web的管理器显示类似以下的信息：

Your update request has been sent. Your database will be updated in a few minutes. Please check your update page for the status of the update. （您的更新请求已被发送，数据库将尽快进行更新。请浏览更新页面查看更新情况。）

几分钟后，如果有可获得的更新，FortiGuard Center系统页面列出新版本的病毒定义信息。系统状态页面也同样显示病毒防护定义的更新日期与版本号。该消息将被记录到时间日志中，标明更新是否成功。

注意：AV与IPS特征需要经常定期进行更新。如果不定期更新AV与IPS特征，FortiGate设备容易受到新病毒的攻击。

使用CLI更新IPS特征

使用CLI接口更新IPS特征。使用以下步骤更新IPS特征：

使用CLI更新IPS特征

1.登录到CLI

2.键入以下CLI命令：

```
configure system autoupdate ips
    set accept-recommended-settings enable
        end
```

制定病毒防护与IPS更新时间

使用基于web的管理器或CLI制定定期、自动更新病毒防护与IPS特征。

使用基于web的管理器制定更新时间

1.进入**系统管理>系统维护> FortiGuard 中心**。

2.点击“制定更新”的功能框。

3.选择以下的更新时间之一并下载更新

Every （每天）24小时之间。选择每次更新间隔的时间。

Daily（每天）您可以指定每天检查更新的时间。

Weekly （每周）您可以指定每周检查更新的时间。

4.点击应用。

FortiGate设备将根据新指定的更新时间执行接下来的更新。

只要FortiGate设备执行所制定时间进行更新，更新事件均将被记录都事件日志中。

使用CLI制定更新时间

1.登录CLI。

2.键入以下命令：

```
config system autoupdate schedule
      set day
      set frequency
      set status
      set time
    end
```

举例

```
config system autoupdate schedule
      set update every Sunday
      set frequency weekly
      set status enable
      set time 16:45
    end
```

添加替代的FDN服务器

如果您不能连接到FDN，或您的公司使用自己的FortiGuard服务器提供更新，使用以下操作步骤在基于web的管理器或CLI中添加替代FDN服务器的IP地址。

使用基于web的管理器添加替代的FDN服务器

1.进入**系统管理>系统维护> FortiGuard 中心**。

2.选中“使用替代FDN服务器地址”的功能框。

3.键入有效的FortiGuard 服务器域名或IP地址
4.点击应用。

FortiGate设备检测与替代FDN服务器的连接。
如果FDN设置更改为“连接”状态，说明FortiGate设备与替代FDN服务器建立了连接。

如果FDN保持“无法连接”状态，说明FortiGate设备不能与替代FDN建立连接。请检查是否是FortiGate配置或网络配置设置阻碍了FortiGate设备与替代FDN服务器的连接。

使用CLI添加替代FDN服务器

1.登录CLI。
2.键入以下命令：

```
config system autoupdate override
    set address
    set status
  end
```

FortiGate固件

Fortinet公司定期更新Fortigate设备固件加强其性能与锁定问题并诊断的功能。FortiGate设备注册完成后，便可以从fortinet网站的技术支持中心http://support.fortinet.com 下载FortiGate设备固件。只有具有对系统模块读和写权限的管理员与设备admin 用户可以更改FortiGate设备固件。
本章包括以下内容：

升级为新的固件版本

使用基于web的管理器或CLI升级为新的FortiOS固件版本或者同一固件版本的较新的子版本。

注意：安装固件替代您现行的防病毒与攻击定义。安装固件后，确保防病毒与攻击定义已经更新。。
详细信息，参见*FortiGate设备管理员使用手册*。

注意：执行以下步骤之前，确认您可以登录使用管理员帐户，或拥有系统配置读写权限的管理员帐户。

使用基于web的管理器升级固件

1. 将固件镜像文件拷贝到您的管理计算机
2. 登录基于web的管理器页面
3. 进入**系统管理>系统状态**.
4. **系统选项>固件版本**选项下，点击“升级”。
5. 输入固件镜像文件的路径与文件名，或点击“浏览”查找文件的位置。
6. 点击OK确认。
FortiGate设备上传固件镜像文件、升级到新的固件版本、重新启动并显示FortiGate登录页面。该操作过程将花费几分钟的时间。
7. 登录基于web的管理器。
8. 进入**系统管理>系统状态，**并检查固件版本确认新固件升级成功
9. 升级防病毒与攻击定义。有关升级防病毒与攻击定义的详细信息，参见*FortiGate设备管理员使用手册*。

使用CLI升级固件
使用以下步骤时，您须配备一台FortiGate设备能够连接到的TFTP服务器。

注意：新的固件安装后将替代您现行的防病毒与攻击定义。因此，新的固件安装完成后，请进行更新防病毒与攻击定义。您也可以使用CLI命令execute update-now进行防病毒与攻击定义的更新。
详细信息，参见*FortiGate设备管理员使用手册*。

注意：执行以下步骤，您必须使用管理员帐户，或拥有系统配置读写权限的管理员帐户登录设备。

使用CLI升级固件

1.确定TFTP服务器已运行。
2.将新的固件镜像拷贝到TFTP服务器的根目录。
3.登录CLI。
4.确定FortiGate设备能够连接到TFTP服务器。
您可以ping一下FortiGate设备是否连接到TFTP服务器。例如，如果TFTP服务器的IP地址是192.168.1.168，那么执行以下命令：
execute ping 192.168.1.168
5.输入以下命令将固件镜像从TFTP服务器拷贝到FortiGate设备：
execute restore image <name_str> <tftp_ip4>
<name_str>输入固件镜像名称，<tftp_ip>输入TFTP服务器的IP地址。
例如：如果固件镜像文件名称是FGT_3000-v3.0-build183-FORTINET.out，TFTP服务器的IP地址是192.168.1.168，那么输入：
execute restore image FGT_3000-v3.0-build183-FORTINET.out 192.168.1.168
FortiGate设备显示以下信息：
This operation will replace the current firmware version! Do you want to continue? (y/n)
6.键入y（是）。
FortiGate设备上传固件镜像文件，升级到新的固件版本并重新启动。该操作过程将花费几分钟时间。
7.重新连接到CLI。
8.确认固件镜像安装成功，输入
get system status
9.升级防病毒与攻击定义（参见*FortiGate设备管理员使用手册*）或进入CLI输入：
execute update-now

恢复为旧的固件版本

以下操作可以将FortiGate设备固件恢复到旧的版本。
使用基于web的管理器或CLI操作可以恢复为旧的固件版本。该操作将FortiGate设备恢复为出厂默认配置。

使用基于web的管理器恢复为旧的固件版本

以下操作将FortiGate设备恢复为出厂默认的配置并删除IPS自定义特征、网页内容列表、邮件过滤列表以及对替换信息所作的修改。
执行该操作之前，建议您：
- 备份FortiGate设备配置。
- 备份IPS自定义特征。
- 备份网页内容与邮件过滤列表。

详细信息，参见*FortiGate设备管理员使用手册*。
恢复为旧的FortiOS版本（例如，从FortiOSv3.0恢复到FortiOSv2.80版本），从备份的配置文件中，不能恢复旧版本的配置。

使用基于web的管理器恢复为旧的固件版本

1. 拷贝固件镜像到管理计算机
2. 登录到FortiGate基于web的管理器
3. 进入**系统管理>系统状态**。
4. 在**系统信息>固件版本**菜单项下，点击“升级”。
5. 键入固件镜像文件的路径与文件名，或点击“浏览”查找文件。
6. 点击OK确认。

FortiGate设备上传固件镜像文件，恢复为旧的固件版本，重新设置配置并重新启动，同时显示FortiGate登录页面。该操作过程将花费几分钟时间实现。

注意：新的固件安装后将替代设备现运行的防病毒与攻击定义。新的固件安装成功后，请下载更新防病毒与攻击定义。
详细信息，参见*FortiGate设备管理员使用手册*。

注意：执行以下步骤，您必须先登录使用管理员帐户，或拥有系统配置读写权限的管理员帐户。

7. 登录基于web的管理器。
8. 进入**系统管理>系统状态**并检查固件版本，确认固件安装成功。
9. 恢复配置。

有关恢复配置的详细信息，参见*FortiGate设备管理员使用手册*。

10. 更新防病毒与攻击定义。

有关防病毒与攻击定义更新的详细信息，参见*FortiGate设备管理员使用手册*。

使用CLI恢复为旧的固件版本

该操作将FortiGate设备恢复为出厂默认的配置，并删除IPS自定义特征，网页内容列表，邮件过滤列表以及对替换信息所作的修改。
执行该操作之前，建议您：
- 使用命令`execute backup config`备份FortiGate设备系统配置
- 使用命令`execute backupipsuserdefsig`备份FortiGate设备系统配置
- 备份网页内容与邮件过滤列表

详细信息，参见*FortiGate设备管理员使用手册*。

恢复为旧的FortiOS版本（例如，从FortiOSv3.0恢复到FortiOSv2.80版本），从备份的配置文件中，不能恢复旧版本的配置。

注意：安装固件替代您现行的防病毒与攻击定义。安装您的固件后，确保防病毒与攻击定义已经更新。您也可以使用CLI命令execute update-now进行防病毒与攻击定义的更新。
详细信息，参见*FortiGate设备管理员使用手册*。

注意：执行以下步骤，您必须先登录使用管理员帐户，或拥有系统配置读写权限的管理员帐户。

执行以下操作，您须配备一台FortiGate设备可以连接到的TFTP服务器。

使用CLI恢复为旧的固件版本

1.确定TFTP服务器已运行。
2.拷贝固件镜像文件到TFTP服务器的根目录。
3.登录到CLI。
4.确定FortiGate设备能够连接到TFTP服务器。
您可以ping一下FortiGate设备是否连接到TFTP服务器。
例如，如果TFTP服务器的IP地址是192.168.1.168，那么执行以下命令：
```
execute ping 192.168.1.168
```
5.输入以下命令将固件镜像从TFTP服务器拷贝到FortiGate设备：
```
execute restore image <name_str> <tftp_ip4>
```
<name_str>输入固件镜像名称，<tftp_ip>输入TFTP服务器的IP地址。
例如：如果固件镜像文件名称是FGT_3000-v3.0-build183-FORTINET.out，TFTP服务器的IP地址是192.168.1.168，那么输入：
```
execute restore image FGT_3000-v3.0-build183-FORTINET.out
192.168.1.168
```
FortiGate设备显示以下提示信息：
```
This operation will replace the current firmware version!
Do you want to continue? (y/n)
```
6.键入y。
FortiGate设备上传固件镜像文件。文件上传之后，类似以下的提示信息显示：
```
Get image from tftp server OK.
Check image OK.
This operation will downgrade the current firmware version!
Do you want to continue? (y/n)
```
7.键入y。
FortiGate设备恢复到旧的固件版本、恢复为出厂默认设置并重新启动。该操作过程将花费几分钟时间。
8.重新连接到CLI。
9. 输入命令`get system status`，确认新的固件镜像已经安装。
10.如需要，使用命令execute restore config<name_str><tftp_ip4>恢复为以前配置。
11.更新防病毒与攻击定义
详细信息，参见*FortiGate设备管理员使用手册*，或在CLI中输入execute update-now。

使用CLI在系统重启过程中安装固件镜像

该操作可以安装指定的固件镜像并将FortiGate设备恢复为默认的设置。您可以使用该操作升级为新的固件版本、恢复为旧的固件版本或重新安装现运行的固件版本。如要执行以上所述操作，您须使用FortiGate console端口与交叉线连接到CLI。该操作将FortiGate设备恢复为出厂默认的配置。

注意：不同的版本的FortiGate BIOS中这一操作略有不同。这些不同将在向牵涉的步骤中说明。 重启FortiGate设备时，BIOS版本号会在Console连接的命令行中显示。

执行该操作时，您需要：

- 使用交叉线连接到FortiGate console控制台接口，访问CLI。
- 安装一台您能够从FortiGate内部接口连接到的TFTP服务器。TFTP服务器应与内部接口处于同一子网中。

执行该操作前，建议您：

- 备份FortiGate设备配置
- 备份IPS自定义特征
- 备份网页内容与邮件过滤

详细信息，参见*FortiGate设备管理员使用手册*。

恢复为旧的FortiOS版本（例如，从FortiOSv3.0恢复到FortiOSv2.80版本），从备份的配置文件中，不能恢复旧版本的配置。

系统重新启动过程中安装固件

1. 使用交叉线与FortiGate console端口连接到CLI。
2. 确定TFTP服务器已经运行。
3. 新的固件镜像文件拷贝到TFTP服务器的根目录。
4. 确定内部接口与TFTP服务器连接的是同一网络。
5. 使用以下操作ping FortiGate设备是否连接到TFTP服务器。例如，如果TFTP服务器的IP地址是192.168.1.168，执行命令：

```
execute ping 192.168.1.168
```

6. 输入execute reboot命令重新启动FortiGate设备，FortiGate设备显示以下提示信息：

```
This operation will reboot the system!
Do you want to continue? (y/n)
```

7. 键入y

FortiGate设备启动时，显示一系列的系统启动信息。当以下信息之一出现时：

- 运行v2.xBIOS的FortiGate设备

```
Press Any Key To Download Boot Image....
```

- 运行v3.xBIOS的FortiGate设备

```
Press any key to display configuration menu.........
```

按任意键中断系统启动。

注意： 3秒内按任意键。如果您没有按下任意键，FortiGate设备继续重启过程，您须重新登录CLI并重复输入execute reboot命令。

如果您成功中断了重启过程，将显示以下信息之一：

• 运行v2.xBIOS的FortiGate设备

```
Enter TFTP Server Address [192.168.1.168]:
```

转入步骤 9

• 运行v3.xBIOS版本的FortiGate设备

```
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[Q]: Quit menu and continue to boot with default
firmware.
[H]: Display this list of options.
```

输入 G, F, Q, 或 H:

8.键入G从TFTP服务器进入新的固件镜像

显示以下信息：

```
Enter TFTP server address [192.168.1.168]:
```

9.键入TFTP服务器的IP地址并按Enter键：

显示如下信息：

```
Enter Local Address [192.168.1.188]:
```

10.键入FortiGate设备用来连接到TFTP服务器的IP地址。该IP地址可以是与该网络接口连接的任何有效的地址。确定您没有误输入该网络中其他设备的IP地址。

显示一下信息：

```
Enter File Name [image.out]:
```

11.输入固件镜像文件名并按Enter键。

TFTP服务器上传固件镜像到FortiGate设备并显示信息：

• 运行v2.xBIOS的FortiGate设备

```
Do You Want To Save The Image? [Y/n]
```

键入Y

• 运行v3.xBIOS版本的FortiGate设备

```
Save as Default firmware/Run image without saving:[D/R]
```

或

```
Save as Default firmware/Backup firmware/Run image without
saving: [D/B/R]
```

12.键入D

设备安装新的固件镜像并重启启动。安装过程需要持续几分钟时间。

恢复新的固件安装之前的配置

如需要，可以更改内部接口地址。您可以在CLI中执行以下命令：

```
config system interface
    edit internal
        set ip <address_ip4mask>
        set allowaccess {ping https ssh telnet http}
    end
```

更改接口地址后，您可以通过基于web的管理器访问FortiGate设备并

恢复配置。
• 恢复FortiGate设备配置
• 恢复IPS自定义特征
• 恢复网页内容过滤
• 恢复邮件过滤列表
• 升级病毒与攻击定义为最新的版本
详细信息，参见*FortiGate设备管理员使用手册*。
恢复为旧的FortiOS版本（例如，从FortiOSv3.0恢复到FortiOSv2.80版本），从备份的配置文件中，不能恢复旧版本的配置。

安装固件之前测试新的固件镜像

在系统重启过程中安装固件镜像的时候可以检测新的镜像并将其保存在系统内存中。完成该操作后，FortiGate设备以当前配置运行使用新的镜像。新的镜像不是永久性的安装，下次FortiGate设备重启时，将以当前的配置运行使用最初安装的固件镜像。如果新的镜像运行良好，您可以使用46页的“升级为新的固件版本”操作，永久安装使用该镜像。
安装新镜像之前，使用以下操作测试新的固件镜像。执行该操作时，您需要使用FortiGate console接口与一根交叉线连接到CLI。该操作使用当前的配置，暂时性的安装新的固件镜像。
执行该操作时，您需要：
• 使用交叉线与FortiGate console端口连接，访问CLI。
• 安装一台您可以通过FortiGate内部接口连接的TFTP服务器。TFTP服务器应与内部接口处于同一子网。

检测新的固件镜像
1. 使用交叉线与FortiGate console端口连接到CLI。
2. 确定TFTP服务器运行。
3. 将新的固件镜像拷贝到TFTP服务器的根目录。
4. 确认内部接口与TFTP服务器连接的同一网段。
Ping一下FortiGate设备是否连接到TFTP服务器。例如，如果TFTP服务器的IP地址是192.168.1.168，执行命令：
```
execute ping 192.168.1.168
```
5. 输入以下命令重新启动FortiGate设备：
```
execute reboot
```
6. FortiGate设备重启时，按任意键中断系统启动。FortiGate设备重启时，显示一系列的系统启动信息：
• 运行v2.xBIOS的FortiGate设备
```
Press Any Key To Download Boot Image.
```
• 运行v3.xBIOS的FortiGate设备
```
Press any key to display configuration menu.
```
7. 按任意键立即中断系统启动。

 **注意：** 3秒内按任意键将中断设备重新启动。如果您没有按下任意键，FortiGate设备继续重启过程，您须重新登录CLI并重新输入

execute reboot命令。
如果您成功中断启动过程，将显示以下信息之一：
• 运行v2.x BIOS的FortiGate设备
Enter TFTP Server Address: [192.168.1.168]:
转入步骤 9
• 运行v3.x BIOS的FortiGate设备
[G]: Get firmware image from TFTP server.
[F]: Format boot device.
[Q]: Quit menu and continue to boot with default firmware.
[H]: Display this list of options.
输入 G, F, Q, 或 H:
8.键入G从TFTP服务器获得新的固件镜像，显示以下信息：
Enter TFTP server address [192.168.1.168]:
9.输入TFTP服务器的IP地址并按Enter键：
显示如下信息：
Enter Local Address [192.168.1.188]:
10.键入一个FortiGate设备用以连接TFTP服务器的IP地址。
该IP地址须是与TFTP服务器处于同一网段的地址。查看该IP地址，确认没有误输入网络中其他设备的IP地址。
显示以下信息：
Enter File Name [image.out]:
11.输入固件镜像文件名并按Enter键。
TFTP服务器上传固件镜像到FortiGate设备并显示信息：
• 运行v2.x BIOS的FortiGate设备
Do You Want To Save The Image? [Y/n]
键入n
• 运行v3.x BIOS的FortiGate设备
Save as Default firmware/Run image without saving: [D/R]
或
Save as Default firmware/Backup firmware/Run image without saving: [D/B/R]
12. 键入R
FortiGate镜像安装在系统内存中，FortiGate设备以当前的配置启动运行新的固件镜像。
13.您可以使用任何管理帐户登录到CLI或基于web的管理器。
14.在CLI中键入get system status确认新的固件镜像已经安装。
如需要，您可以检测新的固件镜像。